Digital rights management in a 3G mobile phone and beyond

Full text Pdf (307 KB)

Source **ACM Workshop On Digital Rights Management** archive
Proceedings of the 3rd ACM workshop on Digital rights management table of contents
Washington, DC, USA
SESSION: DRM experience table of contents
Pages: 27 - 38
Year of Publication: 2003
ISBN:1-58113-786-9

Authors Thomas S. Messerges Motorola Labs, Schaumburg, IL
Ezzat A. Dabbish Motorola Labs, Schaumburg, IL

Sponsors ACM: Association for Computing Machinery
SIGSAC: ACM Special Interest Group on Security, Audit, and Control

Publisher ACM Press New York, NY, USA

↑ ABSTRACT

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management is introduced. Our new approach uses key sharing to help alleviate bad user experiences that are associated with some rights management systems. Examples outlining the enrollment of devices and the acquisition, rendering, and superdistribution of content are shown. Our proposed system is not only applicable to a mobile phone system, but may also be extended to other embedded systems, such as personal digital assistants, set-top boxes, or personal computers.

↑ REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 3GPP TS 23.057, "3rd Generation Partnership Project; Technical Specification Group Terminals; Mobile Station Application Execution Environment (MExE); Functional description; Stage 2; (Release 4)".

2 3GPP TS 23.140, "Multimedia Messaging Service (MMS); Functional description; Stage 2".

3 "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001, Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

4 Shigeo Araki, The Memory Stick, IEEE Micro, v.20 n.4, p.40-46, July 2000

5 Pravin Bhagwat, Bluetooth: Technology for Short-Range Wireless Apps, IEEE Internet Computing, v.5 n.3, p.96-103, May 2001

6 Willms Buhse, Implications of Digital Rights Management for Online Music - A Business Perspective, Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, p.201-212, November 05, 2001

7 Business Software Alliance Report, Available: http://www.bsa.org/.

8 Steven M. Cherry, Media: making music pay, IEEE Spectrum, v.38 n.10, p.41-46, October 2001

9 Future Mobile Phones--Complex Design Challenges from an Embedded Systems Perspective, Proceedings of the Seventh International Conference on Engineering of Complex Computer Systems, p.92, June 11-13, 2001

10 K. Enoki, "i-mode: The Mobile Internet Service of the 21st Century," IEEE International Solid-State Circuits Conference (ISSCC), 2001, pp. 12--5.

11 Joan Feigenbaum , Michael J. Freedman , Tomas Sander , Adam Shostack, Privacy Engineering for Digital Rights Management Systems, Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, p.76-105, November 05, 2001

12 Xianjun Geng , Andrew B. Whinston, Profiting from Value-Added Wireless Services, Computer, v.34 n.8, p.87-89, August 2001

13 GSM 02.09 (ETS 300 506), "Digital Cellular Telecommunications System (Phase 2); Security Aspects," Aug. 2000.

14 Anita Hamilton, "The Pirates of Prime Time," Time.com, Feb. 16, 2002, Available: http://www.time.com/time/business/article/0,8599,203498,00.html.

15 F. Hartung and F. Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications," IEEE Communications Magazine, vol. 38, issue 11, Nov. 2000, pp. 78--84.

16 "International Federation of the Phonographic Industry (IFPI) Music Piracy Report," June 2002, Available: http://www.ifpi.org/site-content/library/piracy2002.pdf.

17 International Intellectual Property Alliance, "USTR 2002 'Special 301' Decisions and Estimated Trade Losses Due to Copyright Piracy," April 30, 2002, Available: http://www.iipa.com/pdf/2002_Apr30_USTRLOSSES.pdf.

18 "JSR-000118 Mobile Information Device Profile Public Review Draft Specification 2.0," Available at: http://java.sun.com.

19 Jupiter Media Metrix - Press Release, "Subscriptions Will Account For Almost Two-Thirds Of US Digital Music Sales In 2006," Jan. 15, 2002, Available: http://www.jmm.com/xp/jmm/press/2002/pr_011502.xml.

20 N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, 1987, pp. 203--9.

21 David W. Kravitz , Kim-Ee Yeoh , Nicol So, Secure Open Systems for Protecting Privacy and Digital Services, Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, p.106-125, November 05, 2001

22 The Internet is changing the music industry, Communications of the ACM, v.44 n.8, p.62-68, Aug. 2001

23 B.M. Macq and J.-J. Quisquater, "Cryptology for Digital TV Broadcasting," Proceedings of the IEEE , vol. 83, issue 6 , June 1995, pp. 944--57.

24 Anna Wilde Mathews, Martin Peers and Nick Wingfield, "Music Industry Finally Online - But Listeners Stay Away in Droves," Wall Street Journal, May 7, 2002.

25 Ryoichi Mori and Masaji Kawahara, "Superdistribution: The Concept and the Architecture," The Transactions of the IEICE, vol. E 73, no. 7, July 1990.

26 Walter S Mossberg, "Sony's Digital Music Clip is Cool, but Treats Users Like Criminals," Wall Street Journal, March 2nd, 2000.

27 M.W. Oliphant, "The Mobile Phone Meets the Internet," IEEE Spectrum, vol. 36, issue 8, Aug. 1999, pp. 20--8.

28 Benny Pinkas, Efficient State Updates for Key Management, Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, p.40-56, November 05, 2001

29 "Piracy Blamed for CD Sales Slump," BBC News, Feb. 26, 2002, Available: http://news.bbc.co.uk/hi/english/entertainment/new_media/newsid_1841000/1841768.stm

30 R. L. Rivest , A. Shamir , L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, v.21 n.2, p.120-126, Feb. 1978

31 William Rosenblatt , Stephen Mooney , William Trippe, Digital Rights Management: Business and Technology, John Wiley & Sons, Inc., New York, NY, 2001

32 Tomas Sander, Golden Times for Digital Rights Management?, Proceedings of the 5th International Conference on Financial Cryptography, p.64-74, February 19-22, 2002

33 P.B. Schneck, "Persistent Access Control to Prevent Piracy of Digital Information," Proceedings of the IEEE, vol. 87 issue 7, July 1999, pp. 1239--50.

34 Secure Digital Music Initiative (SDMI), "SDMI Portable Device Specification," Part 1, ver. 1.0, 1999.

35 "Secure Hash Standard (SHS)," FIPS PUB 180-1, April 1995, Available at: http://www.itl.nist.gov/fipspubs/fip180-1.htm.

36 See http://odrl.net.

37 See: http://www.gnutella.com/.

38 See http://www.keitaide-music.org/.

39 See: http://www.musiccity.com/.

40 See: http://www.openmobilealliance.org/.

41 See http://www.xrml.org.

42 Mark Stefik, "Letting Loose the Light: Igniting Commerce in Electronic Publication," in Internet Dreams, Mark Stefik ed., MIT Press, 1997, pp. 219--254.

43 Richard Stern, Napster: A Walking Copyright Infringement?, IEEE Micro, v.20 n.6, p.4-5, 95, November 2000

44 Wireless Application Protocol, Available: http://www.wapforum.org/.

↑ CITED BY

Reihaneh Safavi-Naini , Nicholas Paul Sheppard , Takeyuki Uehara, Import/export in digital rights management, Proceedings of the 4th ACM workshop on Digital rights management, October 25-25, 2004, Washington DC, USA

↑ INDEX TERMS

Primary Classification:

D. Software

↳ **D.4** OPERATING SYSTEMS

↳ **D.4.6** Security and Protection

↳ **Subjects:** Access controls

Additional Classification:

K. Computing Milieux

↳ **K.6** MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS

↳ **K.6.5** Security and Protection (D.4.6, K.4.2)

↳ **Subjects:** Unauthorized access (e.g., hacking, phreaking)

General Terms:

Design, Security

Keywords:

MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

↑ Collaborative Colleagues:

Ezzat A. Dabbish:	Thomas S. Messerges Robert H. Sloan
Thomas S. Messerges:	Ed Callaway Johnas Cukier Ezzat A. Dabbish Ezzy A. Dabbish Tom A. M. Kevenaar Larry Puhl Robert Sloan Robert H. Sloan René Struik

↑ Peer to Peer - Readers of this Article have also read:

- Web application security assessment by fault injection and behavior monitoring **Proceedings of the 12th international conference on World Wide Web**
  Yao-Wen Huang , Shih-Kun Huang , Tsung-Po Lin , Chung-Hung Tsai

- Data structures for quadtree approximation and compression **Communications of the ACM** 28, 9
  Hanan Samet

- A hierarchical single-key-lock access control using the Chinese remainder theorem **Proceedings of the 1992 ACM/SIGAPP Symposium on Applied computing**
  Kim S. Lee , Huizhu Lu , D. D. Fisher

- The GemStone object database management system **Communications of the ACM** 34, 10
  Paul Butterworth , Allen Otis , Jacob Stein

- Putting innovation to work: adoption strategies for multimedia communication systems **Communications of the ACM** 34, 12
  Ellen Francik , Susan Ehrlich Rudman , Donna Cooper , Stephen Levine

Published before October 2003
Terms used **open mobile alliance** and **drm**

Found **3** of **147,506**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 3 of 3

Relevance scale

1 Cryptography and competition policy: issues with 'trusted computing'

Ross Anderson
July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing PODC '03**
Publisher: ACM Press

Full text available: pdf(991.66 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The most significant strategic development in information technology over the past year has been 'trusted computing'. This is popularly associated with Microsoft's 'Palladium' project, recently renamed 'NGSCB'. In this paper, I give an outline of the technical aspects of 'trusted computing' and sketch some of the public policy consequences.

2 Identification control: Owner-controlled information

Carrie Gates, Jacob Slonim
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press

Full text available: pdf(1.06 MB) Additional Information: full citation, abstract, references

Information about individuals is currently maintained in many thousands of databases, with much of that information, such as name and address, replicated across multiple databases. However, this proliferation of personal information raises issues of privacy for the individual, as well as maintenance issues in terms of the accuracy of the information. Ideally, each individual would own, maintain and control his personal information, allowing access to those who needed at the time it was needed. O ...

Keywords: architecture, privacy, security

3 Processor microarchitecture II: AEGIS: architecture for tamper-evident and tamper-resistant processing

G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas
June 2003 **Proceedings of the 17th annual international conference on Supercomputing ICS '03**
Publisher: ACM Press

Full text available: pdf(286.90 KB) Additional Information: full citation, abstract, references, citings, index

terms

We describe the architecture for a single-chip aegis processor which can be used to build computing systems secure against both physical and software attacks. Our architecture assumes that all components external to the processor, such as memory, are untrusted. We show two different implementations. In the first case, the core functionality of the operating system is trusted and implemented in a security kernel. We also describe a variant implementation assuming an untrusted operating s ...

Keywords: certified execution, secure processors, software licensing

Results 1 - 3 of 3